भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

राज्य सभा

अतारांकित प्रश्न संख्या 722

जिसका उत्तर 24 जुलाई, 2026 को दिया जाना है ।

02 श्रावण, 1948 (शक)

साइबर सुरक्षा तंत्र को सुदृढ़ बनाना

722. श्री के. आर. एन. राजेश कुमारः

क्या **इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी** मंत्री यह बताने की कृपा करेंगे किः

(क)क्या सरकारी संस्थाओं पर साइबर हमलों की संख्या में वृद्धि हुई है;

(ख)यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(ग) क्या भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) द्वारा साइबर सुरक्षा तंत्र को सुदृढ़ किया गया है; और

(घ) इस संबंध में की गई कार्रवाई का ब्यौरा क्या है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से (घ): भारत सरकार की नीतियों का उद्देश्य देश में उपयोगकर्ताओं के लिए खुला, सुरक्षित, विश्वसनीय और जवाबदेह साइबर स्पेस सुनिश्चित करना है। सरकार सरकारी संस्थानों के सामने आने वाले विभिन्न साइबर सुरक्षा खतरों और चुनौतियों से अवगत है।सरकार ने देश में साइबर सुरक्षा तंत्र को सुदृढ़ करने के लिए अनेक उपाय किए हैं, जिनमें अन्य बातों के साथ-साथ निम्नलिखित शामिल हैं:

i. **भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन)** को सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70बी के प्रावधानों के तहत साइबर सुरक्षा घटनाओं पर कार्रवाई करने के लिए राष्ट्रीय एजेंसी के रूप में नामित किया गया है।

ii. सर्ट-इन प्रभावित संगठनों, सेवा प्रदाताओं, नियामकों और कानून प्रवर्तन एजेंसियों के साथ घटना प्रतिक्रिया उपायों का समन्वय करता है।

iii. सर्ट-इन द्वारा कार्यान्वित **राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी),** साइबर सुरक्षा खतरों का पता लगाने के लिए साइबरस्पेस की जांच करता है। यह कार्रवाई करने के लिए संबंधित संगठनों, राज्य सरकारों और हितधारक एजेंसियों के साथ जानकारी साझा करता है।

iv. सर्ट-इन एक स्वचालित साइबर खतरे की खुफिया जानकारी साझा करने वाला मंच संचालित करता है, जिसका उपयोग विभिन्न क्षेत्रों के संगठनों के साथ अनुकूलित अलर्ट साझा करने और खतरों को पहले से ही कम करने के लिए किया जाता है।

v. **साइबर स्वच्छता केंद्र (सीएसके)**

- सर्ट-इन द्वारा प्रदान की जाने वाली एक नागरिक-केंद्रित सेवा, जो स्वच्छ भारत के दृष्टिकोण को साइबर स्पेस तक विस्तारित करती है।
- यह बॉटनेट क्लीनिंग एंड मैलवेयर एनालिसिस सेंटर है और दुर्भावनापूर्ण कार्यक्रमों का पता लगाने में मदद करता है और इसे हटाने के लिए निःशुल्क टूल प्रदान करता है।
- यह नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम अभ्यास भी प्रदान करता है।

vi. **सेक्टोरल कंप्यूटर सुरक्षा घटना प्रतिक्रिया दल (सीएसआईआरटी)**

- बैंकिंग और वित्तीय क्षेत्र में साइबर घटना प्रतिक्रिया के समन्वय के लिए सर्ट-इन के तहत वित्त क्षेत्र में सीएसआईआरटी (सीएसआईआरटी-फिन) मई 2020 से चालू है।
- सीएसआईआरटी-पावर सितंबर 2024 से बिजली क्षेत्र की संस्थाओं के भीतर साइबर सुरक्षा के मुद्दों के समन्वय के लिए सर्ट-इन की एक विस्तारित शाखा के रूप में काम कर रहा है।

vii. सर्ट-इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और ऑडिट करने के लिए 237 सुरक्षा ऑडिटिंग संगठनों को सूचीबद्ध किया है।

viii. सर्ट-इन ने सभी मंत्रालयों/विभागों, राज्य सरकारों और उनके संगठनों द्वारा कार्यान्वयन के लिए साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक साइबर संकट प्रबंधन योजना (सीसीएमपी) तैयार की है।

ix. साइबर सुरक्षा की स्थिति और सरकारी और महत्वपूर्ण क्षेत्रों में संगठनों की तैयारियों का आकलन करने में सक्षम बनाने के लिए सर्ट-इन द्वारा नियमित रूप से साइबर सुरक्षा मॉक ड्रिल आयोजित की जाती है।

x. सर्ट-इन ने सॉफ्टवेयर/उपकरणों में कमजोरियों को ठीक करने के लिए शोधकर्ताओं/अन्वेषण करनेवालों / विक्रेताओं के साथ संग्रह, विश्लेषण, शमन और समन्वय के लिए एक जिम्मेदार भेद्यता प्रकटीकरण और समन्वय कार्यक्रम संचालित किया है।

xi. सर्ट-इन कंप्यूटर, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों/कमजोरियों और प्रतिउपायों के बारे में अलर्ट और सलाह जारी करता है।

xii. सर्ट-इन सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों के आईटी/साइबर सुरक्षा पेशेवरों के लिए नियमित साइबर सुरक्षा प्रशिक्षण, कार्यशालाएं आयोजित करता है।

xiii. **सलाह, दिशानिर्देश और निर्देश**

- सर्ट-इन ने मई 2026 में "डिजिटल इंफ्रास्ट्रक्चर में एआई-आधारित कमज़ोरियों के फ़ायदा उठाने से बचाव और जोखिम कम करने के लिए ब्लूप्रिंट" जारी किया है। इसका उद्देश्य तेज़ी से बदलते एआई-संचालित साइबर खतरों से डिजिटल इंफ्रास्ट्रक्चर की सुरक्षा करना है।
- सर्ट-इन ने अप्रैल 2026 में "फ्रंटियर एआई संचालित साइबर जोखिमों से बचाव" शीर्षक से एक एडवाइजरी जारी की है, जिसमें उन्नत एआई-सक्षम खतरों के खिलाफ सुरक्षा को मजबूत करने के लिए संगठनों और व्यक्तियों के लिए व्यापक उपायों की रूपरेखा तैयार की गई है।
- सर्ट-इन ने सॉफ्टवेयर, हार्डवेयर, आर्टिफिशियल इंटेलिजेंस, क्वांटम कंप्यूटिंग और क्रिप्टोग्राफी आवश्यकताओं के लिए बिल ऑफ मैटेरियल्स (बीओएम) के लिए जुलाई 2025 में अद्यतन तकनीकी दिशानिर्देश जारी किए हैं।
- सर्ट-इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा प्रथाओं पर दिशानिर्देश जारी किए हैं, जिसमें डेटा सुरक्षा, नेटवर्क सुरक्षा, पहचान और पहुंच प्रबंधन, एप्लिकेशन सुरक्षा, तृतीय-पक्ष आउटसोर्सिंग, सख्त प्रक्रियाएं, सुरक्षा निगरानी, घटना प्रबंधन और सुरक्षा ऑडिटिंग जैसे डोमेन शामिल हैं।
- सर्ट-इन ने अप्रैल 2022 में सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70बी की उप-धारा (6) के अंतर्गत सुरक्षित और विश्वसनीय इंटरनेट के लिए साइबर घटनाओं की सूचना सुरक्षा प्रथाओं, प्रक्रिया, रोकथाम, प्रतिक्रिया और रिपोर्टिंग से संबंधित साइबर सुरक्षा निर्देश जारी किए हैं।

****